基于数字列表分发的量子检测拜占庭协议设计与分析

颜世露[1], 张俊勃[2,3], 齐洪胜[4,5], 崔 巍[1,3†]

(1. 华南理工大学 自动化科学与工程学院, 广东 广州 510640; 2. 华南理工大学 电力学院, 广东 广州 510640;
3. 琶洲实验室, 广东 广州 510335; 4. 中国科学院数学与系统科学研究院 系统控制重点实验室, 北京 100190;
5. 中国科学院大学 数学学院, 北京 100049)

摘要: 量子科技有望赋能区块链技术, 提升区块链共识机制的安全性能. 根据是否存在诚实独立的量子源设备, 本文提出了两种可用于多个节点的高成功率的数字列表分发方法, 并进一步提出了一种新的基于数字列表分发的量子检测拜占庭协议. 4个节点的共识示例验证了提出的协议符合检测拜占庭协议的条件. 最后通过分析和比较说明了提出的协议具有较好的实用性和安全性. 与其他协议相比, 本文提出的共识协议不仅能用于解决包含多个节点的区块链系统对多比特数据进行共识的问题, 并能在共识过程中应对任意多恶意节点的攻击, 提高了区块链系统的安全性.

关键词: 区块链; 量子科技; 数字列表分发; 拜占庭协议

引用格式: 颜世露, 张俊勃, 齐洪胜, 等. 基于数字列表分发的量子检测拜占庭协议设计与分析. 控制理论与应用, 2024, 41(8): 1314 – 1324

DOI: 10.7641/CTA.2023.21004

Design and analysis of quantum detectable Byzantine protocol based on numerical list distribution

YAN Shi-lu[1], ZHANG Jun-bo[2,3], QI Hong-sheng[4,5], CUI Wei[1,3†]

(1. College of Automation Science and Technology, South China University of Technology, Guangzhou Guangdong 510640, China;
2. School of Electric Power Engineering, South China University of Technology, Guangzhou Guangdong 510640, China;
3. Pazhou Laboratory, Guangzhou Guangdong 510335, China;
4. Key Laboratory of Systems and Control, Academy of Mathematics and Systems Science,
Chinese Academy of Sciences, Beijing 100190, China;
5. School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Quantum technology can empower blockchain technology and improve the security performance of the blockchain consensus protocol. According to whether there is an honest independent quantum source device (QSD), we propose two numerical list distribution methods with high success rate for multiple nodes, and further propose a new quantum detection Byzantine protocol based on numerical list distribution. A consensus example of four nodes verifies that the proposed protocol meets the conditions for detecting Byzantine protocols. Finally, through analysis and comparison, the proposed protocol has better practicability and security. Compared with other protocols, the consensus protocol proposed in this paper can not only solve the problem of multi-bit data consensus in the blockchain system containing multiple nodes, but also deal with the attack of any number of malicious nodes during the consensus process, which improves the security of the blockchain system.

Key words: blockchain; quantum technology; numerical list distribution; Byzantine agreement

Citation: YAN Shilu, ZHANG Junbo, QI Hongsheng, et al. Design and analysis of quantum detectable Byzantine protocol based on numerical list distribution. *Control Theory & Applications*, 2024, 41(8): 1314 – 1324

1 引言

区块链是通过共识协议保证节点间账本数据一致、通过密码学保证交易数据不可篡改与发送安全的点对点(集体维护、去中心化)的分布式数据库系统. 与中心化系统相比, 去中心化的区块链技术有着更高的可信透明度、容错性和抗攻击性, 并被广泛应用到

收稿日期: 2022−11−13; 录用日期: 2023−11−27.
†通信作者. E-mail: aucuiwei@scut.edu.cn; Tel.: +86 20-87111289.
本文责任编委: 郑子彬.
国家重点研发计划项目(2022YFB3103100), 国家自然科学基金项目(62273154)资助.
Supported by the National Key Research and Development Program of China (2022YFB3103100) and the National Natural Science Foundation of China (62273154).

金融、医疗、能源、溯源等多个领域. 区块链在发展过程中, 面临的制约因素主要有交易处理性能限制、扩展性限制、易用性限制、跨链互联限制、存储限制、缺乏严格数学证明、缺乏形式化证明、区块同步限制、治理与监管限制、软件升级分叉限制等. 共识算法的性能及效率是其中的重要难题. 该难题和文献[1]提出的拜占庭将军问题本质上是一致的: 在已知有将军是叛徒的情况下, 其余诚实的将军如何达成一致行动. 拜占庭将军问题的解可称作拜占庭协议, 也就是设计满足以下2个条件的协议: 1) 所有诚实的将军执行同一个计划; 2) 如果指挥官是诚实的, 那么所有诚实的将军都遵守指挥官所制定的行动计划.

针对原始拜占庭将军问题, 存在着拜占庭将军论断: 将军们在口头同步通信(没有预设其他前提条件)的情况下, 如果叛徒将军的数量大于或等于将军总数的1/3, 则拜占庭将军问题无解[1–2]. 文献[3]通过放松拜占庭协议的条件, 提出一种原始拜占庭将军问题的变种问题—检测的拜占庭将军问题, 并且给出相应的量子检测拜占庭协议, 从而打破拜占庭将军论断的约束. 检测的拜占庭协议是指: 1) 所有诚实的将军要么执行相同的计划, 要么终止行动; 2) 如果指挥官是诚实的, 那么每个诚实的将军要么执行指挥官所制定的计划, 要么终止行动.

经过多年的发展, 学者们已经提出了不少量子检测拜占庭协议[3–16]. 这些协议大都可看作是通过分发和应用数字列表来达成各位将军之间的一致行动的, 其中分发数字列表的方法主要有: 基于三体三维单重量子态[3]、基于四量子比特单重量子态[4]、基于四量子比特纠缠态[6–7]、基于3个或者两个量子密钥分发信道[5]、利用Hardy争论问题[10]、引入一组半诚实的列表分发器[15]等; 而应用数字列表达成共识主要依靠各节点数字列表的互不可见性和数字之间的特定关联属性. 虽然已经提出了许多量子检测拜占庭协议, 但它们一般只考虑了最简单的3个节点的情形, 并且共识内容为单个比特(1表示进攻, 0表示撤退). 而实际的分布式网络和区块链系统通常需要在多个节点之间实现多比特数据共识. 文献[8, 11, 14–16]考虑了多于3个节点的情形, 但文献[8, 14]中协议的前提是系统中恶意节点的数量须少于节点总数的1/3; 文献[11]能容纳任意多的恶意节点, 但其数字列表方法是概率性的, 并且每次分发数字的成功率不高, 因此会造成量子通信资源的浪费; 文献[15]提出基于量子秘钥分发的没有涉及量子纠缠的协议, 但实际上低维纠缠量子态往往更能提高量子秘钥分发的分发效率. 文献[16]的协议仅考虑了存在独立诚实量子源设备时的情景, 去中心化程度有所降低. 所以, 目前仍然缺少在多节点区块链系统中实现对多比特数据共识的安全高效的协议研究. 针对上述问题, 结合已有的一些关于量子算法和区块链的研究工作[17–24], 本文旨在研究可用于区块链系统的、能应对任意多恶意节点攻击的量子检测拜占庭协议.

本文结构如下: 第2节介绍文献[6]中提出的用于三方(3个节点)的量子检测拜占庭协议(GBKCW协议), 说明其如何通过分发和应用数字列表以使得3个节点达成对一个二进制数(0或1)的共识(本文中亦称三节点比特共识); 第3节根据是否存在诚实独立的量子源设备(quantum source device, QSD), 提出两个不同的可用于多个节点的数字列表分发方法; 第4节基于第3节提出的数字列表分发方法对第2节中的GBKCW协议进行改进和拓展, 提出一种新的量子检测拜占庭协议. 4个节点的数据共识示例说明了协议的原理以及验证了提出的协议符合检测拜占庭协议的条件; 第5节通过分析和比较, 说明提出的协议具有实用性和安全性. 与其他协议相比, 提出的协议不仅能用于解决包含多个节点的区块链系统对多比特数据进行共识的问题, 并能在共识过程中应对任意多恶意节点的攻击; 第6节是本文小结.

2　三节点比特共识

文献[6]提出了用于3个节点的量子检测拜占庭协议, 下面对其原理进行简单的介绍. 假设网络中存在3个节点: 主节点P_1和普通节点P_2, P_3, 3个节点分发到的数字列表分别为l_1, l_2和l_3. 这3个列表具有以下关联属性: 1) 3个节点的列表长度都是L. P_1的数字列表l_1中的任一元素都属于集合$\{0,1,2\}$, P_2和P_3的数字列表l_2和l_3中的任一元素都属于集合$\{0,1\}$; 2) 对于3个节点的数字列表的第j位数字, 其组合可能为000, 111, 201, 210这4种情况; 3) 除了能从自己的数字列表中根据性质1和性质2推断出的内容, 任意一个节点都不知道其他节点数字列表的其他内容. 假设各节点分发到的数字列表是$\{l_1$:{2,0,1,0,1,1,2,0,2}, l_2:{0,0,1,0,1,1,0,0,1}, l_3:{1,0,1,0,1,1,1,0,0 }}. 3个节点需要对$m=0$进行共识, 对于每个节点而言, 共识结果只有两种可能: 达成或者放弃对m的共识.

在GBKCW协议中, 首先, P_1给P_2和P_3发送共识消息. 如果P_1是诚实的, 则P_1给P_2发送的m_{12}以及给P_3发送的m_{13}满足m_{12}=$m_{13}=0$. 同时, P_1给P_2, P_3分别发送位置数据列表v_{12}和v_{13}, v_{12}和v_{13}分别包含了l_1中出现比特m_{12}和m_{13}的所有位置, 如这里是$v_{12}=v_{13}=(2,4,8)$. 当P_2收到m_{12}和v_{12}时, P_2检查m_{12}在自身的列表l_2中的位置和v_{12}所描述是否一致, 有以下两种可能:

1) m_{12}, v_{12}和l_2数据一致;

2) m_{12}, v_{12}和l_2数据不一致, P_2确认P_1是恶意节点. 例如此时P_2收到$m_{12}=0$, $v_{12}=(2,4,6)$;

接着, P_2和P_3需要将自己收到的消息相互传输交换. 此处以P_2给P_3发送消息m_{23}为例, m_{23}不仅可以

为0或者1, 还可以为“⊥”, 表示“我收到了不一致的数据”. 而如果P_2收到的消息为0或者1, 他需要发送给P_3一些必要的数据来表明$m_{23}=m_{12}$. 为了达成此目的, P_2同样发送一个位置数据列表v_{23}给P_3, 并且声称这与从P_1处收到的v_{12}一样. 当P_3收到来自P_2的m_{23}, v_{23}或者“⊥”, 他手头早已收到来自P_1的m_{13}和v_{13}.

最后, 对于P_3而言, 来自P_1的信息, 有以下2种情况:

1) $A_1: m_{13}, v_{13}, l_3$数据一致, 即$m_{13}=0, v_{13}=(2,4,8)$;

2) $A_2: m_{13}, v_{13}, l_3$数据不一致, 即“⊥”.

对于P_3而言, 来自P_2的信息, 有以下4种情况:

1) B_1: m_{23}, v_{23}, l_3数据一致, 且$m_{23}=m_{13}=0$, $v_{23}=v_{13}=(2,4,8)$;

2) B_2: m_{23}, v_{23}, l_3数据一致, 且$m_{23}\neq m_{13}$;

3) B_3: “⊥”, 即P_2告诉P_3, 他知道P_1是恶意节点;

4) B_4: m_{23}, v_{23}, l_3数据不一致.

下面对以上情况进行排列组合, 对于节点P_3而言, P_3拿到的信息有8种可能, 根据不同的可能情况可以得到相应的比特共识结果.

1) 如果是A_1B_1, P_3确认没有恶意节点, P_3达成了该轮比特共识m_{13}.

2) 如果是A_1B_2, P_3确认P_1是恶意节点, P_3放弃该轮比特共识m_{13}.

3) 如果是A_1B_3, P_3认为P_2可能是恶意节点, P_3达成该轮比特共识m_{13}.

4) 如果是A_1B_4, P_3确认P_2为恶意节点, P_3达成该轮比特共识m_{13}.

5) 如果是A_2B_1, P_3确认P_1是恶意节点, P_3放弃该轮比特共识m_{13}.

6) 如果是A_2B_2, P_3确认P_1是恶意节点, P_3放弃该轮比特共识m_{13}.

7) 如果是A_2B_3, P_3确认P_1是恶意节点, P_3放弃该轮比特共识m_{13}.

8) 如果是A_2B_4, P_3确认P_1是恶意节点, P_3放弃该轮比特共识m_{13}.

由以上8种可能出现的情况可知, 对于比特m的共识, 只有A_1B_1, A_1B_3, A_1B_4这3种情况会使P_3达成对m的共识, 其余的情况都会使P_3放弃对m的共识. 同理, P_2和P_3具有对称关系, 对于P_3出现的情况也适用于P_2.

3 可用于多节点的数字列表分发方法

根据是否存在诚实独立的QSD, 本节主要提出了两个不同的可用于多个节点的数字列表分发方法. 文献[6]中用于3个节点的数字列表分发方法中, 首先制备四比特量子纠缠态

$$|\phi\rangle=\frac{1}{2\sqrt{3}}(2|0011\rangle-|0101\rangle-|0110\rangle-|1001\rangle-|1010\rangle+2|1100\rangle), \tag{1}$$

接着把量子态$|\phi\rangle$的第1和第2个量子比特分发给主节点, 第3和第4个比特分别分发给其他2个节点. 对于主节点, 定义$|00\rangle$表示1, $|11\rangle$表示0, 其他情况表示2. 3个节点对分发给自己的量子态进行测量即可得到所需的数字. 但是该方法仅仅适用于3个节点. 要将其扩展到n个节点的情形, 可以通过具有以下性质的数字列表来实现:

1) 性质1 : 每个节点的列表长度都是L. P_1的列表l_1中的任一元素都属于集合$\{0,1,2,\cdots,n-1\}$. 其他节点的数字列表$l_2, l_3, \cdots, l_n$中的任一元素都属于集合$\{0,1\}$;

2) 性质2 : 对于每个列表的第j位, 具有下面的关系, 一旦l_1第j位为0(或者1), 那么其他列表对应位置也全是0(或者1). 如果l_1第j位数字用x表示, 且$x\in\{2,\cdots,n-1\}$, 剩下列表第j位数字相加和模n为$n-x$;

3) 性质3 : 除了能从自己的数字列表中根据性质1和性质2推断出的内容, 任意一个节点都不知道其他节点数字列表的其他内容.

下面分别基于量子纠缠态和量子相位估计算法提出了两种可分发具有以上性质的数字列表的方法.

3.1 基于量子纠缠态的数字列表分发方法

假设区块链通信网络中存在n个节点($\log_2 n$为整数), 同时存在一个诚实独立的QSD. 每个节点都和QSD建立起量子通信信道, 能够安全传输量子态. 首先QSD制备L个相同的量子纠缠态

$$|\psi\rangle=\frac{1}{\sqrt{2^{n-1}}}\Big(\sum_{i=0}^{2^{n-1}-1}|i\rangle\otimes\sum_{r=0}^{n-1}|r\rangle\Big),$$
$$\text{s.t. }\Big(\sum_{j=1}^{n}i_j+r\Big)\bmod n=0, \tag{2}$$

其中$i_j\in\{0,1\}$是整数i的$n-1$位二进制表示形式的第j位, $j=1,2,\cdots,n-1$. 对于每个由$\log_2 n+n-1$个量子比特组成的量子态$|\psi\rangle$, QSD给节点P_1分发最后的$\log_2 n$个比特(即式(2)中的量子态$|r\rangle$), 给节点P_k分发第$k-1$个比特, $k\in\{2,3,\cdots,n\}$. 节点P_k在计算基矢上测量分发到的量子比特, 如果测量结果为1, 表明量子比特处于$|0\rangle$, 往数字列表l_k中添加0; 如果测量结果为−1, 表明量子比特处于$|1\rangle$, 往数字列表l_k中添加1. 同样地, 节点P_1在计算基矢上测量分发到的量子态$|r\rangle$, 然后把数字r添加到数字列表l_1中, $r\in\{0,1,\cdots,n-1\}$. 当L个量子态都分发完成, 各节点之间可得到满足性质1、性质2和性质3的数字列表.

基于量子纠缠态的数字列表分发方法伪代码如算法1(见表1)所示, 方法的通信复杂度为$\mathrm{O}(nL)$. 该种方法适用于系统中存在诚实独立的量子源设备. 根据纠缠的性质可知, 只要成功制备量子态$|\psi\rangle$, 数字列表成功分发的概率为1.

表 1 算法1: 基于量子纠缠态的数字列表分发方法

Table 1 Algorithm 1: A numerical list distribution method based on quantum entangled states

Data: 诚实独立的QSD, 选举出主节点P_1, 并确定好数字列表长度$L(L>>n)$;
Result: 节点生成具有性质1、性质2和性质3的一组数字列表;
while $L>0$ **do**
  QSD使用$\log_2 n+n-1$个比特制备量子态$|\psi\rangle$, 然后给P_1分发$|\psi\rangle$的后$\log_2 n$ 个比特; 节点P_1测量分发到的量子态, 根据测量结果, 得到数字r, 并把r 添加到数字列表l_1;
  for $k \Leftarrow 2, n$ **do**
    QSD给节点P_k分发$|\psi\rangle$的第$k-1$个比特; 节点P_k测量分发到的量子比特, 并将测量结果添加到数字列表l_k;
  end
  $L \Leftarrow L-1$
end

3.2 基于量子相位估计的数字列表分发方法

假设区块链通信网络中存在n个节点, 每个节点都具备幺正操作的能力, 下面通过图1展现网络中各节点如何通过量子信道协助实现量子相位估计算法以完成数字列表分发. 图1(a)是下面步骤1–7的量子线路图, 其中的虚线框操作细节如图1(b)所示, 图1(b)也是步骤3–5的量子线路图，其中带箭头波浪线表示量子信道, 其中

$$U=\mathrm{diag}\{\exp(\boldsymbol{i}\frac{2\pi}{n}(N_1+N_2+\cdots+N_n)),1\},$$

节点P_1是数字列表的发起人. 具体步骤如下:

步骤 1　节点P_1从集合$\{0,1,\cdots,n-1\}$中任意选取一个基数N_1; $P_2,P_3,\cdots,P_n$从$\{0,1\}$中分别任意选取基数$N_2,N_3,\cdots,N_n$. 每个节点的基数只有自己知道, 对于其他节点是不可见和不可预测的;

步骤 2　节点P_1使用1个工作比特和t个辅助比特制备初始量子态

$$|\psi_0\rangle=\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^t-1}|s\rangle\otimes|0\rangle; \tag{3}$$

步骤 3　如图1(a)所示, 以辅助量子态的第t位(从上到下)比特为控制位, 以工作比特(最下面的比特)为目标位, P_1应用受控操作$CU_{N_1}^{2^0}$到$|\psi_0\rangle$上, 其中

$$U_{N_1}=\begin{bmatrix}\mathrm{e}^{\boldsymbol{i}\frac{2\pi}{n}N_1} & 0\\ 0 & 1\end{bmatrix}. \tag{4}$$

这样就可以得到如下量子态:

$$|\psi_1\rangle=\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^{t-1}-1}|s\rangle\otimes(|0\rangle+\mathrm{e}^{\boldsymbol{i}\frac{2\pi}{n}N_1}|1\rangle)\otimes|0\rangle, \tag{5}$$

然后节点P_1通过量子信道将$|\psi_1\rangle$传给节点P_2;

步骤 4　以辅助量子态的第t位比特(从上到下)为控制位, 以工作比特(最下面的比特)为目标位, P_2作用受控操作$CU_{N_2}^{2^0}$ 到$|\psi_1\rangle$上, 得到第二量子态

$$|\psi_2\rangle=\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^{t-1}-1}|s\rangle\otimes(|0\rangle+\mathrm{e}^{\boldsymbol{i}\frac{2\pi}{n}(N_1+N_2)}|1\rangle)\otimes|0\rangle, \tag{6}$$

然后通过量子信道将$|\psi_2\rangle$传给普通节点P_3;

步骤 5　节点$P_3,P_4,\cdots,P_n$重复节点P_2的做法, 作用到量子态上的受控操作分别为$CU_{N_3}^{2^0}$, $CU_{N_4}^{2^0}$, $\cdots$, $CU_{N_n}^{2^0}$.节点P_n操作后, 得到第n量子态

$$|\psi_n\rangle=\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^{t-1}-1}|s\rangle\otimes(|0\rangle+\mathrm{e}^{\boldsymbol{i}\frac{2\pi}{n}(N_1+N_2+\cdots+N_n)}|1\rangle)\otimes|0\rangle, \tag{7}$$

此时, 节点P_n通过量子信道将$|\psi_n\rangle$重新传回给主节点P_1;

步骤 6　重复$t-1$次步骤3–5的过程: 对于第j次, $j\in\{1,\cdots,t-1\}$, 每个节点P_k的操作变为受控旋转操作$CU_{N_k}^{2^j}$, 控制位为第$t-j$ 位比特(从上到下), 目标位为工作比特;

步骤 7　通过以上步骤, 节点P_1可得到量子态

$$\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^t-1}\mathrm{e}^{\boldsymbol{i}2\pi\theta s}|s\rangle\otimes|0\rangle, \tag{8}$$

其中$\theta=\dfrac{1}{n}\sum_{k=1}^{n}N_k$. 此时忽略工作比特, P_1对t个辅助比特进行量子傅里叶逆变换操作$\mathrm{FT}^\dagger$,

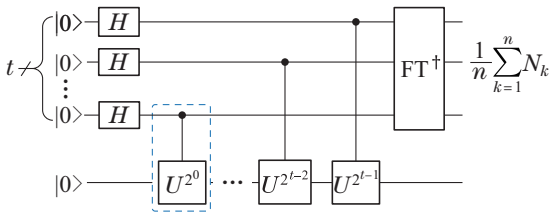
$$\mathrm{FT}^\dagger:\frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^t-1}\mathrm{e}^{\boldsymbol{i}2\pi\theta s}|s\rangle\mapsto|\tilde{\theta}\rangle, \tag{9}$$

得到量子态$|\tilde{\theta}\rangle$. 其中$\widetilde{\theta}$是对θ的近似, 至少能以$1-\varepsilon$的近似成功概率精确到$t-\lceil\log(2+\dfrac{1}{2\varepsilon})\rceil$位[25], ε为误差. P_1选择合适的补充数字N_s使$\sum_{\mathrm{k}=1}^{n}N_k+N_s=0 \bmod n$, 更新

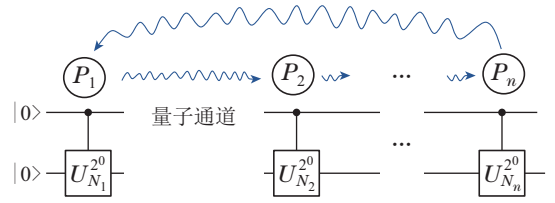
$$N_1=(N_1+N_s)\bmod n. \tag{10}$$

经过以上过程, 每个节点相当于确定了自己拥有的数字列表的1位数字. 重复L次步骤1–7的过程, 节点之间生成了满足性质1、性质2和性质3的数字列表.

基于量子相位估计的数字列表分发方法伪代码如算法2(见表2)所示, 算法的通信复杂度为$\mathrm{O}(ntL)$. 该种方法适用于系统中不存在诚实独立的QSD, 但需要系统中所有节点在数字列表分发过程中都遵循分发过程中的操作规则, 在此前提条件下, 数字列表成功分发的概率为$1-\sigma$, 其中σ为进行L次量子相位估计算法所产生的误差.



(a) 步骤1–7的量子线路图



(b) 步骤3–5的量子线路图

图 1 基于量子相位估计的数字列表分发过程

Fig. 1 Numerical list distribution process based on quantum phase estimation

4 基于数字列表分发的量子检测拜占庭协议

4.1 量子检测拜占庭协议

基于以上提出的数字列表分发方法以及三节点比特共识, 本节提出一种新的量子检测拜占庭协议, 其伪代码如算法 3 (见表 3) 所示. 假设区块链网络中存在n个节点, 节点间需要共识的区块数据为B, B对应的二进制摘要信息可表示为多比特数据$m = m^{(1)}m^{(2)}\cdots m^{(q)}$, $m^{(j)} \in \{0,1\}, j \in \{1,2,\cdots,q\}$, q表示m的二进制长度. 摘要信息是实现区块数据完整性保护的主要工具, 它是由哈希算法运算得到, 具有保护账本数据免受未授权修改和检测区块是否被篡改的能力. 因而, 共识摘要信息等价于共识相应的数据量庞大的区块数据. 节点对每一个二进制数$m^{(j)}$的n节点比特共识都需要使用一次第3节中提出的数字列表分发方法. 协议中, 首先需要选取主节点P_1, 然后按照次序进行q轮的n节点比特共识, 第j轮的n节点比特共识可分为以下两个步骤:

步骤 1 通过第3.1节或第3.2节中的数字列表分发方法给各节点P_k分发用于共识数据m中第j个比特$m^{(j)}$的数字列表$l_k^{(j)}, k \in \{1,2,\cdots,n\}$;

步骤 2 $P_k(k \neq 1)$和P_1, P_k'组成3个节点, 对于$m^{(j)}$进行三节点比特共识, P_k得出达成还是放弃该轮三节点比特共识的结果, 其中$k' \in \{1,2,\cdots,n\}$, 且$k' \neq 1, k$.

可知, 要在n个节点中对m达成共识, 至少需要在n个节点间分发q次长度为L的数字列表以及按次序进行q轮n节点比特共识, 其中每一轮的n节点比特共识可由$n-2$轮三节点比特共识组成. 在P_k和P_1, P_k'组成三节点并进行第j轮的三节点比特共识过程中, 根据第2节中8种情况的表示方法, 约定节点P_k第j轮三节点比特共识结果表示为$R_{k1k'}^j \in \{A_1B_1, A_1B_2, A_1B_3, A_1B_4, A_2B_1, A_2B_2, A_2B_3, A_2B_4\}$, 同时约定达成共识表示为1, 放弃共识表示为0, 则$R_{k1k'}^j \in \{0,1\}$. P_k对数据m的共识结果可表示为

$$\prod_{j=1}^{q}\prod_{k'=2,k'\neq k}^{n} R_{k1k'}^j, \tag{11}$$

若P_k计算式(11)的结果等于1, 则P_k达成对m的共识, 否则放弃对m的共识, 并将相应区块数据写入本地数据库, 否则放弃对m的共识.

表 2 算法2: 基于量子相位估计的数字列表分发方法

Table 2 Algorithm 2: A numerical list distribution method based on quantum phase estimation

Data: 选举出主节点P_1, 并确定好数字列表长度L $(L >> n)$;
Result: 节点生成具有性质1、性质2和性质3的一组数字列表;

while $L > 0$ **do**
  P_1 制备量子态$|\psi_0\rangle$, 并从$\{0,1,\cdots,n-1\}$中任意选取N_1;
  $P_2, P_3, \cdots, P_n$ 从 $\{0,1\}$ 中分别选取 $N_2, N_3, \cdots,$ N_n;
  for $j \Leftarrow 0, t-1$ **do**
    for $k \Leftarrow 1, n$ **do**
      以辅助比特的第$t-j$位比特为控制位, 工作比特为目标位, P_k实施操作$CU_{N_k}^{2^j}$; **if** $k \equiv n$ **then**
        P_k将量子态传给P_1;
      end
      else
        P_k将量子态传给P_{k+1};
      end
    end
  end
  P_1对t位辅助比特进行量子傅里叶逆变换FT†, 得到$\frac{1}{n}\sum_{k=1}^{n} N_k$的近似值

$$\mathrm{FT}^\dagger : \frac{1}{\sqrt{2^t}}\sum_{s=0}^{2^t-1} \mathrm{e}^{\boldsymbol{i}2\pi\theta s}|s\rangle \mapsto |\tilde{\theta}\rangle$$

  P_1从$\{0,1,\cdots,n-1\}$中选取N_s, 使满足

$$(\sum_{k=1}^{n} N_k + N_s) \bmod n = 0$$

  $N_1 \Leftarrow (N_1 + N_s) \bmod n$
  for $k \Leftarrow 1, n$ **do**
    数字列表l_k添加元素N_k
  end
  $L \Leftarrow L - 1$
end

表 3 算法3: 基于数字列表分发的量子检测拜占庭协议

Table 3 Algorithm 3: Byzantine protocol for quantum detection based on numerical list distribution

Data: 选举出主节点P_1, P_1决定共识的数据m(二进制长度为q);
Result: 每个节点达成或者放弃对m的共识;
for $j \Leftarrow 1, q$ **do**
  通过数字列表分发方法得到一组数字列表$l^{(j)}$, 每个节点拥有其中一个列表;
  for $k \Leftarrow 2, n$ **do**
    for $k' \Leftarrow 2, n$ **do**
      if $k \neq k'$ **then**
        P_k和P_1, $P_{k'}$组成3个节点, 根据分发得到的数字列表, 进行三节点比特共识, 并记录比特共识结果$R^j_{k1k'}$;
      end
    end
  end
end
for $k \Leftarrow 2, n$ **do**
  if $\prod_{j=1}^{q}\prod_{k'=2,k'\neq k}^{n} R^j_{k1k'} = 1$ **then**
    P_k达成对m的共识, 并将相应的区块数据写入本地数据库
  end
  else
    P_k放弃共识m
  end
end

为了更好说明量子检测拜占庭协议的原理以及验证协议的正确性, 本节通过举例说明如何在$n = 4$个节点的情况下, 应用提出的量子检测拜占庭协议. 假设各节点共识第1位二进制数时, 分发的数字列表为{l_1: { 2,0,1,2,1,0,3}, l_2: { 1,0,1,0,1,0,1}, l_3: { 0,0,1,1,1,0,0}, l_4: { 1,0,1,1,1,0,0 }}. 共识第2位二进制数时, 分发的数字列表为{l_1:{0,2,2,0,1,3,1}, l_2: {0,0,1,0,1,0,1}, l_3: {0,1,0,0,1,1,1}, l_4:{0,1,1,0,1,0,1}}. 在4个节点的区块链系统中, 可能会出现0,1,2,3这4个恶意节点的情况, 其中又可以根据主节点P_1是否是恶意节点再分为2种可能情况. 没有特定说明的情况下, 默认P_1和其他各节点需要共识的数据为01. 区块链网络各节点共识过程和结果如表4–8所示. 对于每个表格, 共有5大行(第1列所在的5行)和5大列(最后1行所在的5 列); 最后1大行表示每个节点的对P_1发送的消息的共识结果; 第2大列表示节点P_1 给其余各节点发送消息; 第3至第5大列表示每3个节点之间进行2轮的三节点比特共识, 包含了消息发送过程和比特共识结果; 星号表示该部分内容不影响协议最终结果(只需考虑诚实节点的共识结果), 可省略; 比特共识结果$R^1_{213}=1(A_1B_1)$表示由P_2, P_1, P_3组成的三节点比特共识中, P_2共识第1位比特的结果为1(即达成共识), 对应第2节中的8种可能情况中的A_1B_1.

容易知道, 存在3个恶意节点时(即只有一个诚实节点), 无论哪个节点是诚实节点, 唯一的诚实节点总会达成诚实且一致的行动. 而4个节点都是恶意节点的时候根本不用考虑诚实节点的行为. 在表6和表8中, P_1是恶意节点, 还可能会出现P_1发送的比特和比特对应位置列表不一致的情况. 但根据提出的协议内容, 在该种情况下, 诚实的节点最终会放弃共识. 综合表4–8的结果, 可以指出, 在包含4个节点的区块链系统中, 无论系统中存在多少恶意节点, 对于主节点发起的区块数据共识, 本文设计的量子检测拜占庭协议满足以下两个条件:

条件 1　所有诚实的节点要么达成对相同的区块数据的共识, 并将区块数据写入本地数据库, 要么放弃共识;

条件 2　如果主节点是诚实的, 则所有诚实节点要么达成对主节点发送的区块数据的共识, 并将该区块数据写入本地数据库, 要么放弃共识.

同理, 本文提出的量子检测拜占庭协议也能扩展应用到$n > 4$的情景. 因而, 本文提出的量子检测拜占庭协议符合检测拜占庭协议的条件.

4.2 量子区块链系统

当前已经出现了很多不同体系结构的区块链系统, 但这些区块链系统在技术基础架构上仍有较多的共性. 在经典区块链技术基础架构的启发下, 本节展示了一种潜在的新型量子区块链系统, 其技术架构自下而上大致可以分为用户层、核心层、基础层3层结构. 用户层由节点管理和业务功能组成, 主要负责用各类用户(节点)认证接入、退出、权限验证及控制、各种业务和功能说明等. 核心层由量子检测拜占庭协议、智能合约和抗量子攻击加密算法组成, 量子检测拜占庭协议实现各节点在特定时间内和不可信的网络环境中达成一致; 智能合约负责将区块链系统的业务逻辑以代码的形式实现、编译并部署, 完成既定规则的条件触发和自动执行; 抗量子攻击加密算法为上层组件提供密码学算法支持, 包括各种哈希算法、签名算法、隐私保护算法等. 基础层由计算存储和对等网络组成, 可使用QCPU, CPU, GPU, ASIC等完成系统各种计算任务, 使用硬盘等存储资源存储区块链计算和上链等信息, 以及使用量子信道和经典信道实现各节点间的通信互联.

区块链系统设计普遍存在“区块链不可能三角”的局限, 也就是其无法同时兼顾“去中心化”、“可扩展性”和“安全性”三者. 比如工作量证明机制[26]能容纳

少于50%的恶意节点, 但牺牲了可扩展性, 且交易处理效率较低; 实用拜占庭容错协议[27]支持恶意节点数量不超过1/3总节点数的情形, 性能较高, 但扩展性差; Raft算法[28]使区块链系统接近于传统分布式数据库的主流性能水平, 但却不支持拜占庭容错. 虽然本文提出的量子检测拜占庭协议一定程度上也受到“区块链不可能三角”的限制, 但如果系统可能会出现任意多的恶意节点, 那么本文提出的协议能作为一种插拔式的共识协议应用到区块链的核心层中, 进而构建能应对任意多恶意节点攻击的新型量子区块链系统, 并通过第4.2节中所描述的共识过程来保证节点间的数据一致性.

5 分析与比较

本文提出的可应用于区块链系统的量子检测拜占庭协议主要分为两个阶段: 第1阶段是满足特定性质的数字列表的分发阶段; 第2阶段是应用数字列表进行共识的阶段. 除了数字列表分发阶段需要使用量子资源, 提出的协议其他内容都只使用到经典资源, 并且每次数字列表分发成功率接近1, 在含噪声的中型量子计算(noisy intermediate-scale quantum, NISQ)时代只有少量量子资源的情况下显得更有优势. 在复杂度上, 由算法3可知, 协议的量子通信复杂度为$\mathrm{O}(nqL)$或者$\mathrm{O}(ntqL)$(分别对应第3.1节和第3.2节的两个分发方法), 而经典通信复杂度为$\mathrm{O}(n^2q)$, 都属于多项式复杂度. 而多项式复杂度的算法在计算机领域被广泛认为是有效算法, 说明提出的协议具备了实用性的重要前提.

由三节点比特共识的原理及其8种可能的结果可知, 量子检测拜占庭协议的优势在于: 每个诚实节点根据得到的消息, 可以预先确认某个节点是恶意节点或者“认为”某个节点可能是恶意节点, 再做出对主节点发送的内容的共识决定(达成共识或放弃共识), 这也是“检测”的含义. 在协议的安全性上, 攻击者的目的以及攻击成功的标志有2个: 1) 使得诚实节点对于主节点发送的共识消息做出不一致的共识行为(部分诚实节点达成共识, 而其他诚实节点放弃共识); 2) 使得诚实节点的本地数据库内容并不完全一样, 也就是诚实节点之间共识了不一致的内容. 而第4.2节中例子验证了提出的协议满足检测拜占庭检测协议的2个条件, 能够使得所有诚实节点对于P_1发送的消息做出一致的共识行为, 并且如果达成共识, 则所有诚实节点最终会共识一致的内容. 因此, 本文提出的协议是能够阻止攻击者达成其攻击目的.

提出的协议是基于第2节中的三节点比特共识的, 协议共识阶段的安全性由三节点比特共识原理得以保障. 攻击者对协议的攻击手段主要集中于数字列表分发阶段, 尝试通过破坏数字列表的3个性质来达到其攻击目的. 第3.1节中的数字列表分发方法依赖于诚实独立的QSD, QSD本身不会对协议进行攻击, 所以第3.1节中的方法所分发的数字列表必然满足所规定的性质1和性质2. 同时又因为假设了QSD与各节点的量子通信信道能安全可靠地传输量子态, 不会出现量子态被截获重发的情况, 所以第3.1节中的方法所分发的数字列表必然满足所规定的性质3. 对于第3.2节中基于量子相位估计的数字列表分发方法, 如果数字列表分发过程受到攻击并导致分发到的数字列表不满足性质1或性质2, 则会导致诚实节点放弃共识. 例如第3.2节的方法依赖于各节点遵循分发过程中的操作规则, 一旦存在恶意节点不遵守指定的操作规则, 根据量子相位估计算法的计算原理, 会使得主节点在执行式(9)后得到的相位结果并不是预期的值, 所以分发的数字列表不会满足性质2. 此时诚实节点是可以在共识阶段是根据三节点比特共识原理检测出存在恶意行为, 诚实节点最终不会对不一致的消息达成共识, 也就是会放弃共识. 然而在该种情况下, 诚实节点判断不了到底是数字列表分发阶段还是共识阶段出现了恶意行为, 以及“检测”不了哪个节点是恶意节点. 恶意节点也会考虑通过破坏数字列表的性质3来达到其攻击目的, 也就是在量子态传输过程中对量子态进行窃取信息的操作. 但是任何非平凡的操作都会改变原来量子态的信息, 直接导致执行的不再是预期的量子相位估计操作, 进一步使得数字列表不满足性质2, 最后诚实节点也会放弃共识. 而根据量子不可克隆原理, 也排除了节点复制量子态来窃取信息的可能. 因而, 攻击者不能通过破坏数字列表的3个性质来达到前面所述的攻击目的.

当前已经有了不少关于量子检测拜占庭协议的研究和讨论, 本文主要改进和拓展了文献 [6] 提出的GBKCW协议, 进而提出一种能适用于区块链等多节点系统的、有综合性优势的量子检测拜占庭协议. 相对于文献[13], 本文的协议能应对存在任意多恶意节点的情形, 而不仅仅局限于恶意节点数量少于1/3总节点数量时的情形. 相比于文献[11] 提出的概率性数字列表分发方法, 本文协议的优势在于数字列表分发方法是确定性的, 意味着每次量子通信资源的使用都是有效的而不会导致浪费. 文献[16]只考虑了存在诚实独立QSD时的单一情形, 而本文的协议根据是否存在诚实独立的QSD, 分别提出两种能用于多个节点的高成功率的数字列表分发方法, 应用场景更加全面. 同时, 已有的大多数量子检测拜占庭协议一般只讨论如何共识单比特数据, 而本文较为详细地描述了区块链系统应用量子检测拜占庭协议共识多比特数据的过程, 并提出量子区块链技术架构设想, 期望能为未来“量子+区块链”的结合研究提供有用的借鉴和参考.

表 4 0个恶意节点

Table 4 0 malicious nodes

消息接收节点		P_2		P_3		P_4		P_2		P_3		P_4	
消息发送节点		P_1						P_3	P_4	P_2	P_4	P_2	P_3
第1轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=0,$	$m_{42}=0,$	$m_{23}=0,$	$m_{43}=0,$	$m_{24}=0,$	$m_{34}=0,$
		0	$\{2,6\}$	0	$\{2,6\}$	0	$\{2,6\}$	$v_{32}=\{2,6\}$	$v_{42}=\{2,6\}$	$v_{23}=\{2,6\}$	$v_{43}=\{2,6\}$	$v_{24}=\{2,6\}$	$v_{34}=\{2,6\}$
	比特共识结果	—						R^1_{213}	R^1_{214}	R^1_{312}	R^1_{314}	R^1_{412}	R^1_{413}
								$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$
第2轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=1,$	$m_{42}=1,$	$m_{23}=1,$	$m_{43}=1,$	$m_{24}=1,$	$m_{34}=1,$
		1	$\{5,7\}$	1	$\{5,7\}$	1	$\{5,7\}$	$v_{32}=\{5,7\}$	$v_{42}=\{5,7\}$	$v_{23}=\{5,7\}$	$v_{43}=\{5,7\}$	$v_{24}=\{5,7\}$	$v_{34}=\{5,7\}$
	比特共识结果	—						R^2_{213}	R^2_{214}	R^2_{312}	R^2_{314}	R^2_{412}	R^2_{413}
								$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$
对P_1发送的消息的共识结果		P_1达成						P_2达成		P_3达成		P_4达成	

表 5 1个恶意节点: P_4是恶意节点, P_1, P_2, P_3是诚实节点

Table 5 one malicious node: P_4 is a malicious node, P_1, P_2, and P_3 are honest nodes

消息接收节点		P_2		P_3		P_4		P_2		P_3		P_4	
消息发送节点		P_1						P_3	P_4	P_2	P_4	P_2	P_3
第1轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=0, v_{32}=\{2,6\}$	可能发送的消息: 1. $m_{42}=1, v_{42}=\{1,3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	$m_{23}=0, v_{23}=\{2,6\}$	可能发送的消息: 1. $m_{43}=1, v_{43}=\{1,3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*
		0	$\{2,6\}$	0	$\{2,6\}$	0	$\{2,6\}$						
	比特共识结果	—						R^1_{213} $1(A_1B_1)$	R^1_{214} $1(A_1B_3$ 或者$A_1B_4)$	R^1_{312} $1(A_1B_1)$	R^1_{314} $1(A_1B_3$ 或者$A_1B_4)$	R^1_{412} *	R^1_{413} *
第2轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=1, v_{32}=\{5,7\}$	可能发送的消息: 1. $m_{42}=0, v_{42}=\{1,4,6\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	$m_{23}=1, v_{23}=\{5,7\}$	可能发送的消息: 1. $m_{43}=0, v_{43}=\{1,4,6\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*
		1	$\{5,7\}$	1	$\{5,7\}$	1	$\{5,7\}$						
	比特共识结果	—						R^2_{213} $1(A_1B_1)$	R^2_{214} $1(A_1B_3$ 或者$A_1B_4)$	R^2_{312} $1(A_1B_1)$	R^2_{314} $1(A_1B_3$ 或者$A_1B_4)$	R^2_{412} *	R^2_{413} *
对P_1发送的消息的共识结果		P_1达成						P_2达成		P_3达成		*	

表 6 1个恶意节点: P_1是恶意节点, P_2, P_3, P_4是诚实节点, 假设P_1对P_2, P_3发送01, 对P_4发送00

Table 6 One malicious node: P_1 is a malicious node, P_2, P_3 and P_4 are honesst nodes, assuming that P_1 sends 01 to P_2 and P_3, and sends 00 to P_4

消息接收节点		P_2		P_3		P_4		P_2		P_3		P_4	
消息发送节点		P_1						P_3	P_4	P_2	P_4	P_2	P_3
第1轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=0,$	$m_{42}=0,$	$m_{23}=0,$	$m_{43}=0,$	$m_{24}=0,$	$m_{34}=0,$
		0	$\{2,6\}$	0	$\{2,6\}$	0	$\{2,6\}$	$v_{32}=\{2,6\}$	$v_{42}=\{2,6\}$	$v_{23}=\{2,6\}$	$v_{43}=\{2,6\}$	$v_{24}=\{2,6\}$	$v_{34}=\{2,6\}$
	比特共识结果				—			R^1_{213}	R^1_{214}	R^1_{312}	R^1_{314}	R^1_{412}	R^1_{413}
								$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$	$1(A_1B_1)$
第2轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=1,$	$m_{42}=0,$	$m_{23}=1,$	$m_{43}=0,$	$m_{24}=1,$	$m_{34}=1,$
		1	$\{5,7\}$	1	$\{5,7\}$	0	$\{1,4\}$	$v_{32}=\{5,7\}$	$v_{42}=\{1,4\}$	$v_{23}=\{5,7\}$	$v_{43}=\{1,4\}$	$v_{24}=\{5,7\}$	$v_{34}=\{5,7\}$
	比特共识结果				—			R^2_{213}	R^2_{214}	R^2_{312}	R^2_{314}	R^2_{412}	R^2_{413}
								$1(A_1B_1)$	$0(A_1B_2)$	$1(A_1B_1)$	$0(A_1B_2)$	$0(A_1B_2)$	$0(A_1B_2)$
对P_1发送的消息的共识结果		*						P_2放弃		P_3放弃		P_4放弃	

表 7 2个恶意节点: P_3, P_4是恶意节点, P_1, P_2是诚实节点

Table 7 Two malicious nodes: P_3 and P_4 are malicious nodes, P_1 and P_2 are honest nodes

消息接收节点		P_2		P_3		P_4		P_2		P_3		P_4	
消息发送节点		P_1						P_3	P_4	P_2	P_4	P_2	P_3
第1轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	可能发送的消息: 1. $m_{32}=1, v_{32}=\{3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	可能发送的消息: 1. $m_{42}=1, v_{42}=\{1,3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*	*	*
		0	$\{2,6\}$	0	$\{2,6\}$	0	$\{2,6\}$						
	比特共识结果				—			R^1_{213}	R^1_{214}	R^1_{312}	R^1_{314}	R^1_{412}	R^1_{413}
								$1(A_1B_3$ 或者$A_1B_4)$	$1(A_1B_3$ 或者$A_1B_4)$	*	*	*	*
第2轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	可能发送的消息: 1. $m_{32}=0, v_{32}=\{1,3,4\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	可能发送的消息: 1. $m_{42}=0, v_{42}=\{1,4,6\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*	*	*
		1	$\{5,7\}$	1	$\{5,7\}$	1	$\{5,7\}$						
	比特共识结果				—			R^2_{213}	R^2_{214}	R^2_{312}	R^2_{314}	R^2_{412}	R^2_{413}
								$1(A_1B_3$ 或者$A_1B_4)$	$1(A_1B_3$ 或者$A_1B_4)$	*	*	*	*
对P_1发送的消息的共识结果		P_1达成						P_2达成		*		*	

表 8 2个恶意节点: P_1, P_4是恶意节点, P_2, P_3是诚实节点, 假设P_1对P_2发送10, 对P_3发送11, 对P_4发送00

Table 8 Two malicious nodes: P1and P_4 are malicious nodes, P_2 and P_3 are honest nodes, assuming that P_1 sends 10 to P_2, sends 11 to P_3, sends 00 to P_4

消息接收节点		P_2		P_3		P_4		P_2		P_3		P_4	
消息发送节点		P_1						P_3	P_4	P_2	P_4	P_2	P_3
第1轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=1, v_{32}=\{3,5\}$	可能发送的消息: 1. $m_{42}=1, v_{42}=\{1,3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	$m_{23}=1, v_{23}=\{3,5\}$	可能发送的消息: 1. $m_{43}=1, v_{43}=\{1,3,4,5\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*
		1	$\{3,5\}$	1	$\{3,5\}$	0	$\{2,6\}$						
	比特共识结果	—						R_{213}^1 $1(A_1B_1)$	R_{214}^1 $1(A_1B_3$或者(A_1B_4)	R_{312}^1 $1(A_1B_1)$	R_{314}^1 $1(A_1B_3)$或者(A_1B_4)	R_{412}^1 *	R_{413}^1 *
第2轮三节点比特共识	消息传递	m_{12}	v_{12}	m_{13}	v_{13}	m_{14}	v_{14}	$m_{32}=1, v_{32}=\{5,7\}$	可能发送的消息: 1. $m_{42}=1, v_{42}=\{2,3,5,7\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	$m_{23}=0, v_{23}=\{2,4\}$	可能发送的消息: 1. $m_{43}=1, v_{43}=\{2,3,5,7\}$; 2. “$\perp$”; 3. 其他破坏诚实节点达成一致的消息	*	*
		0	$\{2,4\}$	1	$\{5,7\}$	0	$\{2,4\}$						
	比特共识结果	—						R_{213}^2 $0(A_1B_2)$	R_{214}^2 $1(A_1B_3$或者(A_1B_4)	R_{312}^2 $0(A_1B_2)$	R_{314}^2 $1(A_1B_3)$或者(A_1B_4)	R_{412}^2 *	R_{413}^2 *
对P_1发送的消息的共识结果		*						P_2放弃		P_3放弃		*	

6 结论

本文主要针对区块链系统共识过程存在的拜占庭容错问题开展了研究. 根据是否存在诚实独立的QSD, 本文首先提出两种能用于多个节点的高成功率的数字列表分发方法, 进而提出一种新的基于数字列表分发的量子检测拜占庭协议. 4个节点的数据共识示例验证了提出的协议符合检测拜占庭协议的条件. 通过分析和比较, 进一步说明提出的协议具备一定的实用性和安全性. 与其他协议相比, 提出的协议不仅能用于解决包含多个节点的区块链系统对多比特数据进行共识的问题, 并能在共识过程中应对任意多恶意节点的攻击, 提高了区块链系统的安全性.

参考文献:

[1] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 1982, 4(3): 382 – 401.

[2] PEASE M, SHOSTAK R, LAMPORT L. Reaching agreement in the presence of faults. *Journal of the ACM*, 1980, 27(2): 228 – 234.

[3] FITZI M, GISIN N, MAURER U. Quantum solution to the Byzantine agreement problem. *Physical Review Letters*, 2001, 87(21): 217901.

[4] CABELLO A. Solving the liar detection problem using the four-qubit singlet state. *Physical Review A*, 2003, 68(1): 012304.

[5] IBLISDIR S, GISIN N. Byzantine agreement with two quantum-key-distribution setups. *Physical Review A*, 2004, 70(3): 034306.

[6] GAERTNER S, BOURENNANE M, KURTSIEFER C, et al. Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection. *Physical Review Letters*, 2008, 100(7): 070504.

[7] GAO F, GUO F Z, WEN Q Y, et al. Comment on experimental demonstration of a quantum protocol for Byzantine agreement and liar detection. *Physical Review Letters*, 2008, 101(20): 208901.

[8] BEN-OR M, HASSIDIM A. Fast quantum Byzantine agreement. *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. New York, USA: 2005: 481 – 485.

[9] BOURENNANE M, CABELLO A, ZUKOWSKI M. Quantum Byzantine agreement with a single qutrit. *ArXiv Preprint*, 2010, arXiv: 1001.1947.

[10] RAHAMAN R, WIEŚNIAK M, ŻUKOWSKI M. Quantum Byzantine agreement via Hardy correlations and entanglement swapping. *Physical Review A*, 2015, 92(4): 042302.

[11] TAVAKOLI A, CABELLO A, ŻUKOWSKI M, et al. Quantum clock synchronization with a single qudit. *Scientific Reports*, 2015, 5: 7982.

[12] WU Xia, JIA Hengyue, ZHU Jianming. Entangled state testing in the quantum Byzantine agreement. *Chinese Journal of Network and Information Security*, 2016, 2(11): 30 – 38.
(武霞, 贾恒越, 朱建明. 量子拜占庭协议中的纠缠态探测. 网络与信息安全学报, 2016, 2(11): 30 – 38.)

[13] LUO Q B, FENG K Y, ZHENG M H. Quantum multi-valued Byzantine agreement based on d-dimensional entangled states. *International Journal of Theoretical Physics*, 2019, 58(12): 4025 – 4032.

[14] FENG Y, SHI R, ZHOU J, et al. Quantum Byzantine agreement with tripartite entangled states. *International Journal of Theoretical Physics*, 2019, 58(5): 1482 – 1498.

[15] SUN X, KULICKI P, SOPEK M. Multi-party quantum Byzantine agreement without entanglement. *Entropy*, 2020: 22(10): 1152.

[16] CHOLVI V. Detectable quantum Byzantine agreement for any arbitrary number of dishonest parties. *Arxiv Preprint*, 2021, arXiv: 2112.09437v1.

[17] YAN S L, QI H S, CUI W. Nonlinear quantum neuron: A fundamental building block for quantum neural networks. *Physical Review A*, 2020, 102(5): 052421.

[18] CUI W, YAN S L. Module for arbitrary controlled rotation in gate-based quantum algorithms. *Physica A: Statistical Mechanics and Its Applications*, 2023, 626: 129092.

[19] CUI W, DOU T, YAN S L. Threats and opportunities: Blockchain meets quantum computation. *Proceedings of the 39th Chinese Control Conference*. Shenyang, China: IEEE, 2020: 5822 – 5824.

[20] YAN Shilu, XIANG Lipeng, CUI Wei. Opportunities and challenges of Blockchain in the quantum era. *Journal of University of Electronic Science and Technology of China*, 2022, 51(2): 162 – 169.
(颜世露, 相里朋, 崔巍. 区块链在量子时代的机遇和挑战. 电子科技大学学报, 2022, 51(2): 162 – 169.)

[21] QI H S, MU B Q, PETERSEN I R, et al. Measurement-induced Boolean dynamics and controllability for closed quantum networks. *Automatica*, 2020, 114: 108816.

[22] QI H S, MU B Q, PETERSEN I R, et al. Measurement-induced Boolean dynamics for open quantum networks. *IEEE Transactions on Control of Network Systems*, 2023, 10(1): 134 – 146.

[23] WANG W, YU Y, DU L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. *Scientific Report*, 2022, 12: 8606.

[24] YANG Z, SALMAN T, JAIN R, et al. Decentralization using quantum blockchain: A theoretical analysis. *IEEE Transactions on Quantum Engineering*, 2022, 3: 4100716.

[25] NIELSEN M A, CHUANG I. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2002.

[26] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 2008: 21260.

[27] CASTRO M, LISKOV B. Practical Byzantine fault tolerance. *Proceedings of the third symposium on Operating Systems Design and Implementation*. New Orleans, LA: IEEE, 1999: 173 – 186.

[28] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm. *Proceedings of 2014 USENIX Annual Technical Conference*. Philadelphia, PA: USENIX, 2014: 305 – 319.

作者简介:

颜世露 硕士研究生, 目前研究方向为量子神经网络, E-mail: yanshilu@foxmail.com;

张俊勃 教授, 目前研究方向为电力系统及其自动化, E-mail: epjbzhang@scut.edu.cn;

齐洪胜 副研究员, 目前研究方向为布尔网络控制、量子控制, E-mail: qihongsh@amss.ac.cn;

崔 巍 教授, 目前研究方向为单光子视觉、数据治理与区块链安全, E-mail: aucuiwei@scut.edu.cn.